UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, v. CHI PING PATRICK HO, a/k/a/ "Patrick C.P. Ho," a/k/a/ "He Zhiping," Defendant.	:	No. 17 Cr. 779 (KBF)

DEFENDANT'S MEMORANDUM OF LAW
IN SUPPORT OF HIS MOTION TO SUPPRESS

KRIEGER KIM & LEWIN LLP
500 Fifth Avenue, 34th Floor
New York, New York 10110
Tel.: (212) 390-9550

DECHERT LLP
1095 Avenue of the Americas
New York, New York 10036
Tel.: (212) 698-3500
Fax: (212) 698-3599

Attorneys for Chi Ping Patrick Ho

Table of Contents

Table of Authorities

Defendant Chi Ping Patrick Ho ("Dr. Ho") respectfully moves this Court to suppress (1) a post-arrest statement made by Dr. Ho; (2) all evidence obtained from a Huawei cellular telephone recovered from Dr. Ho's luggage; and (3) all of the emails obtained pursuant to search warrants for certain email accounts issued in this case, and all evidence derived therefrom.

Dr. Ho was arrested by Federal Bureau of Investigation ("FBI") agents on Nov. 18, 2017. After being placed into custody, but prior to being read his *Miranda* rights, the agents asked Dr. Ho for the password to an iPad in his possession, explicitly and intentionally misleading him as to the purpose of the request. Dr. Ho acquiesced to the request and provided the password. The FBI then proceeded to use that illegally obtained password to access the contents of *another* device, a cellular telephone, that was also in Dr. Ho's possession at the time of his arrest. The government failed to disclose the *Miranda* violation to the Court in the course of securing the warrant to search the contents of that device. The government also did not inform the Court that it intended to use the illegally obtained password to execute the warrant. In a willful end-run around Dr. Ho's Fourth and Fifth Amendment rights, the government now seeks to use the evidence illegally collected from that second device against Dr. Ho at trial. The Court should accordingly suppress not only the original, illegally obtained statement from Dr. Ho, but also the fruit of that statement, *i.e.*, all evidence collected from the cellular telephone.

The Court should also suppress all emails obtained pursuant to certain search warrants issued in this case. The Fourth Amendment requires the government to review search warrant returns for responsiveness within a "reasonable" period of time. Yet more than twenty-one months after the government first began receiving search warrant returns containing the contents of five email accounts, the government has not completed its responsiveness review. The government has thus retained, for nearly two years, countless personal emails that were not

within the scope of the original search warrants. The government's extraordinary delay in completing even this basic review of the materials exceeds what other courts have expressly held to be unreasonable and in violation of the Fourth Amendment, and it demonstrates a flagrant disregard of the terms of the search warrants. As such, blanket suppression of the emails is not only warranted, but in fact required.

Background

Dr. Ho's Arrest and the Search of His Cellular Telephone

On November 16, 2017, Dr. Ho was charged by sealed complaint with violations of the Foreign Corrupt Practices Act ("FCPA") and money laundering offenses. (*See* Compl., ECF No. 1.) Two days later, he was arrested by FBI agents at John F. Kennedy International Airport ("JFK"), after arriving on a commercial flight for a business trip. *See* Decl. of Edward Y. Kim, Apr. 16, 2018 ("Kim Decl."), Ex. A ("Arrest Log"). At the time of his arrest, agents seized, among other things, a Huawei cellular telephone (the "Cellphone") and iPad (the "iPad") in Dr. Ho's possession. *See* Kim Decl., Ex. B ("Receipt for Property").

After Dr. Ho was arrested and transported to the FBI's JFK facility, but *prior to being read his Miranda rights*, the agents asked Dr. Ho for the password to the iPad. *See* Kim Decl., Ex. C ("FBI 302"). The agents stated that they wanted the password ostensibly "to unlock the iPad for purposes of putting it on airplane mode and shutting it off." *Id.* According to an FBI report documenting the interaction, Dr. Ho provided the password (the "Password"), and the agents unlocked the iPad, turned on airplane mode, and turned off the iPad. *See id.* Dr. Ho was later advised of his *Miranda* rights, at which point he immediately invoked his right to an attorney. *See* Kim Decl., Ex. D ("Advice of Rights Form").

Nearly two months later, on January 10, 2018, the government applied to this Court for a warrant to search, among other things, the Cellphone and the iPad (the "Devices Search Warrant"). *See* Kim Decl., Ex. E ("Appl. and Agent Aff."). In support of the search warrant application, the government submitted a 19-page affidavit from an FBI Special Agent. *See id.* That affidavit set forth the circumstances of Dr. Ho's arrest and that of his co-defendant, Cheikh Gadio. *Id.* ¶¶ 9, 10. The affidavit also noted that, after his arrest, Mr. Gadio had waived his *Miranda* rights and participated in an interview. *Id.* at 11 n.6. However, the agent's affidavit omitted any reference to the fact that Dr. Ho had invoked his *Miranda* rights and that the FBI had obtained the Password after Dr. Ho's arrest but before he was advised of his *Miranda* rights. *See id.* Nor did the government advise the Court that it intended to execute the Devices Search Warrant using the improperly obtained Password. *See id.* Based upon this affidavit, the Court ultimately issued the Devices Search Warrant requested by the government. *See* Kim Decl., Ex. F.

On March 9, 2018, the defense requested that the government advise it "of any instances in which the government has used the [P]assword in any way, including to access the iPad or any other device." Kim Decl., Ex. G at 2 ("Defense's March 9 Letter"). In response to the defense request, the government disclosed—for the first time—that the FBI's Computer Analysis and Response Team had used the Password to "more efficiently access" the Cellphone during the execution of the search warrant for the Cellphone.[1] Kim Decl., Ex. H at 3 ("Government's March 23 Letter").

[1] The Password appears to have been the same for both the iPad and the Cellphone.

The Government's Collection and Review of Emails

In addition to seizing data from electronic devices taken from Dr. Ho and others, the government has also obtained emails from numerous accounts that were the subject of other search warrants (the "Email Search Warrants").[2] On March 2, 2018, the government informed the Court that it had "retained a third-party vendor to assist in the review of all of the emails obtained pursuant to pertinent search warrants . . . and to assist in the process of sorting these returns into emails that are 'identified' as responsive to the relevant warrant(s) and those that are 'not identified' as responsive to the relevant warrant(s)." (Letter to Hon. Katherine B. Forrest at 1-2, Mar. 2, 2018, ECF No. 54.) The government stated that it understood "that the third-party vendor expect[ed] to have completed its initial review within approximately a week." (*Id.* at 2.) It stated that it then intended "to review the vendor's work and confirm the adequacy of the vendor's identification of documents as responsive to the relevant warrant(s), and . . . then process and produce the identified emails to the defense." (*Id.*)

The defense subsequently requested additional information from the government regarding the discovery it had produced, including the review procedure that was used to execute the Email Search Warrants. Specifically, the defense requested the following:

> [F]or each account from which the government has obtained emails pursuant to a search warrant, please provide the following information: (1) the email address associated with the account; (2) the date or dates on which the government obtained emails from the service provider of the account; (3) the dates on which the review of emails from the account began and ended; (4) the dates on which an initial review of the emails from the account was conducted in order to determine which emails were responsive to the search warrant; (5) the procedures used

[2] The email accounts specifically at issue here are: (1) secgen@chinaenergyfund.org; (2) head@chinaenergyfund.org; (3) cpho@chinaenergyfund.org; (4) hocppatrick@gmail.com; and (5) kimosabehk@yahoo.com.uk (the "Email Accounts"). These email accounts were searched pursuant to search warrants issued on June 16, 2016 (16 Mag. 3894), August 4, 2016 (16 Mag. 4694), and October 24, 2016 (16 Mag. 6845).

> to determine which emails were responsive to the search warrant, including any search terms used to limit the scope of the review; (6) the names and roles of the individuals who conducted the review; (7) the procedures used to ensure that members of the case team were walled off from non-responsive and privileged materials; (8) confirmation that members of the case team were not exposed to non-responsive or privileged materials; and (9) the procedures used to ensure that *Brady* and *Giglio* material was properly identified.

Defense's March 9 Letter at 2.

The government responded on March 23, 2018, stating that it "d[id] not agree that [the defense was] entitled to much or all of the information [it sought.]" *See* Government's March 23 Letter at 1. The government noted, however, that it had begun to receive search warrant returns for five email accounts used by Dr. Ho as early as June 20, 2016—roughly *twenty-one months* prior to the date of its letter. *See id.* at 2. The government also noted that for each of the email accounts, "a member of the prosecution team began reviewing the returns within approximately two weeks" of receiving search warrant returns. *See id.* at 2. However, the government's response appears to indicate that, as of the date of its letter, it had still not yet completed its responsiveness review, stating only that "on or about March 23, 2018," the date of its letter, it had instructed its third-party vendor to begin uploading emails "'identified' as responsive" for processing and production. *Id.* The government did not provide any of the other requested information about its review procedure, including, among other things, when its responsiveness review of each email account began and ended and the procedures used in performing a responsiveness review.

Argument

After Dr. Ho was arrested, FBI agents used a three-step process to evade constitutional requirements in order to gain access to the Cellphone. First, agents questioned Dr. Ho after arresting him but prior to giving him *Miranda* warnings—explicitly and intentionally misleading

him as to the purpose of the questioning. Second, agents specifically failed to disclose this *Miranda* violation to the Court in the course of securing a search warrant to search the contents of the Cellphone. Third, and finally, the FBI then used the illegally obtained statement to collect evidence to be used against Dr. Ho at trial. It is difficult to conceive of a law enforcement approach better designed to evade Fourth and Fifth Amendment constitutional requirements. The Court should accordingly suppress Dr. Ho's illegally obtained statement as well as the evidence recovered from the Cellphone.

The Court should also suppress all emails obtained pursuant to the Email Search Warrants, and all evidence derived therefrom, because the government's delay in completing a review for responsiveness has been unreasonable. It has thus shown flagrant disregard of the terms of the search warrants, such that blanket suppression of the search warrant returns is well warranted.

POINT I

THE COURT SHOULD SUPPRESS DR. HO'S STATEMENT AND ALL EVIDENCE OBTAINED FROM THE CELLPHONE[3]

The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U. S. Const. Amend. V. "To protect the Fifth Amendment right against self-incrimination, the Supreme Court in *Miranda v. Arizona* ruled that police may not interrogate a suspect who has been taken into custody without first warning the person 'that he has the right to remain silent, that anything he says can be used against him in a court of law, that he has the right to the presence of an attorney, and that if he cannot afford an attorney one

[3] The government has represented that aside from accessing the iPad to turn it to airplane mode, it has used the Password to access only the Cellphone. To the extent that the government also used the password to access any other devices, these same arguments would apply with respect to any evidence obtained from those devices as well.

will be appointed for him prior to any questioning if he so desires.'" *United States v. Newton*, 369 F.3d 659, 668 (2d Cir. 2004) (quoting *Miranda* v. *Arizona*, 384 U.S. 436, 479 (1966)). Where a suspect is not properly warned of his rights, "the prosecution is barred from using statements obtained during the interrogation to establish its case in chief." *Id.* at 668.

Here, there can be no serious dispute that the agents obtained the Password in violation of *Miranda*. The record is clear that Dr. Ho provided the Password *prior to* being read his *Miranda* rights, in response to questioning *after* being placed under arrest—thus, after he had been taken into custody. *See* FBI 302; *Newton*, 369 F.3d at 670 ("The 'ultimate inquiry' for determining *Miranda* custody . . . is . . . 'whether there is a "formal arrest or restraint on freedom of movement" of the degree associated with a formal arrest.'" (quoting *California v. Beheler*, 463 U.S. 1121, 1125 (1983))). Furthermore, FBI agents asked Dr. Ho a question—under the guise of asking for a way to switch one device (the iPad) into airplane mode—that was designed to elicit information (the Password) from Dr. Ho. The FBI then later used the Password to access *an entirely different* electronic device, all in an effort to obtain additional incriminating evidence against Dr. Ho. Accordingly, the agents' post-arrest questioning of Dr. Ho regarding the Password constituted custodial interrogation under *Miranda*. *See Rhode Island v. Innis*, 446 U.S. 291, 300–01 (1980) ("[T]he *Miranda* safeguards come into play whenever a person in custody is subjected to either express questioning or . . . any words or actions on the part of the police (other than those normally attendant to arrest and custody) that the police should know are reasonably likely to elicit an incriminating response from the suspect."); *Newton*, 369 F.3d at 671 ("*Miranda* itself defined 'custodial interrogation' as 'questioning initiated by law enforcement officers after a person has been taken into custody . . .").

In addition to the foregone conclusion that Dr. Ho's statement regarding the Password must be suppressed, any evidence obtained by means of that statement also must be suppressed.[4] *See United States v. Crews*, 445 U.S. 463, 470 (1980) ("[T]he exclusionary sanction applies to any 'fruits' of a constitutional violation."); *United States v. Hubbell*, 530 U.S. 27, 37-38 (2000) ("[T]he phrase 'in any criminal case' in the text of the Fifth Amendment might have been read to limit its coverage to compelled testimony that is used against the defendant in the trial itself. It has, however, long been settled that its protection encompasses compelled statements that lead to the discovery of incriminating evidence even though the statements themselves are not incriminating and are not introduced into evidence.").

This case thus presents the Court with an obvious violation of *Miranda* that requires suppression of the illegally obtained statement. Equally important, in this case, law enforcement agents violated *Miranda* in order improperly to obtain one of the pieces of information most critical to modern-day investigations: the password to an individual's personal electronic device. The importance of the information obtained through the intentional *Miranda* violation calls for an appropriate remedy. Limiting the remedy in this case to the mere fact of the statement itself would ignore the significance of the Password and would not account for the vast evidentiary benefits that agents sought to obtain by improperly eliciting the Password. Accordingly, the interest in deterring misconduct on the part of law enforcement is particularly critical in this case and warrants suppression of the fruit of the illegally obtained statement.

[4] It is also worth noting that Dr. Ho promptly invoked his right to counsel after being advised of his rights. *See* Advice of Rights Form. Thus, there is every reason to believe that here, had the government advised Dr. Ho of his rights at the proper time, Dr. Ho would in fact not have disclosed his password to the agents. *See United States v. Djibo*, 151 F. Supp. 3d 297, 309 (E.D.N.Y. 2015) ("Djibo invoked the right to remain silent once Officer Wilburt gave him the *Miranda* warnings. One can conclude that he would not have given the passcode had the warning been given on time[.]").

The decision in *United States v. Djibo*, 151 F. Supp. 3d 297 (E.D.N.Y. 2015), is particularly instructive. In that case, the defendant was asked for, and provided, his telephone passcode prior to being read his *Miranda* rights. *See id.* at 299-300. The government used the passcode to unlock the telephone and complete an initial search of it, and then later completed a full forensic search of the phone pursuant to a search warrant. *See id.* at 299-302. The government conceded that the initial search was "a fruit of the un-Mirandized statements," and it consented to the suppression of all evidence obtained pursuant to that search. *See id.* at 307. The government argued, however, that the later search was valid, relying in large part on *United States v. Patane*, 542 U.S. 630 (2004), in which the Supreme Court found that a defendant's voluntary statements obtained in violation of *Miranda* did not necessitate suppression of a gun that was found as the result of those statements.

The *Djibo* court rejected this argument. Among other things, the court stated that discovery of a firearm and discovery of the entire contents of a smart phone are "vastly different searches," with the former implicating only the Fifth Amendment's privilege but the latter invoking the Fourth Amendment's protection against unreasonable searches and seizures. *See Djibo*, 151 F. Supp. 3d at 308-10. The court also rejected the government's argument "that [the defendant's] passcode was not required because [the government] would have inevitably been able to hack the phone." *Id.* at 310. In the end, the court ordered that "any documents obtained by virtue of [the defendant] providing his passcode [be] suppressed as either the fruit of the unlawful inquiry by [the agent] . . . and/or fruit of the admittedly poisonous [initial search]." *Id.*; *see United States v. Gilkeson*, 431 F. Supp. 2d 270, 294 (N.D.N.Y. 2006) (granting motion to suppress derivative evidence as fruit of statements taken in violation of *Miranda*).

As the *Djibo* court concluded, the Supreme Court's holding in *Patane* does not counsel in favor of a different result. In that case, law enforcement officers initially arrested the defendant for violating a restraining order. *Id.* at 635. Officers then began to advise the defendant of his *Miranda* rights, but were interrupted by the defendant, who said that he knew his rights. *Id.* Officers then asked the defendant about a gun they had reason to believe he possessed, and the defendant eventually revealed the location of the gun and gave officers permission to retrieve it. *Id.* Officers then recovered the gun, which the defendant later moved to suppress. *Id.*

The Court reversed a decision to suppress the gun and remanded for further proceedings. *Id.* at 637. In reaching this conclusion, the Court noted that while it need not define the boundaries of Fifth Amendment protections, with respect to failures to advise defendants of their *Miranda* rights, there was "nothing to deter" and there was therefore no reason to suppress the physical fruits of such *Miranda* violations. *Id.* at 637, 642. Notably, *Patane* involved a good faith attempt by agents to administer *Miranda* rights. *Id.* at 635.

Consistent with the holding in *Djibo*, this Court should reject any argument that the holding of *Patane* extends to situations in which agents have purposefully solicited statements in violation of *Miranda* to then obtain access to electronic devices. *Patane* addressed a situation in which statements obtained in technical violation of the *Miranda* strictures led to the recovery of the fruit itself—the gun. By contrast, in this case, the fruit of an intentional violation—the Password—led to untold quantities of additional information from a different electronic device than the one that was supposed to be placed in airplane mode.

Particularly in these circumstances, interpreting *Patane* to apply to the search of electronic devices would lead to untenable consequences. Given modern-day encryption technology, a holding that *Patane* applies to the search of electronic devices would create

powerful incentives for law enforcement agents illegally to obtain passwords for devices that might otherwise fall outside the reach of law enforcement. Indeed, the entire point of eliciting such statements is the password itself. That is, the forbidden statement has an intrinsic value wholly different from other statements that might lead to physical evidence. Failing to suppress the fruit of such violations would undermine one of the fundamental premises of the holding in *Patane*—namely, that there is "nothing to deter" with respect to failures to warn. *See Patane*, 542 U.S. at 641. As courts have increasingly recognized, the contents of modern-day electronic devices are so vast—and searches thereof so invasive—that they must be accorded heightened protection. *See, e.g., United States v. Galpin*, 720 F.3d 436, 446-47 (2d Cir. 2013) ("Advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain."); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010); *Djibo*, 151 F. Supp. 3d at 310 ("[A] cell phone is not just a physical object containing information. It is more personal than a purse or a wallet, and certainly more so than the firearm that was used in evidence against Respondent *Patane*. It is the combined footprint of what has been occurring socially, economically, personally, psychologically, spiritually and sometimes even sexually, in the owner's life, and it pinpoints the whereabouts of the owner over time with greater precision than any tool heretofore used by law enforcement without aid of a warrant. In today's modern world, a cell phone passcode is the proverbial 'key to a man's kingdom.'"). *But see United States v. Holland*, No. 15-cr-00666, 2016 WL 6068020 (D.S.C. Oct. 17, 2016) (extending the holding of *Patane* to situations in which agents have accessed electronic devices); *United States v. Stark*, No. 09-cr- 20317, 2009 WL 3672103 (E.D. Mich. Nov. 2, 2009) (same);

Report and Recommendation at 10-11, *United States v. Jackson*, 17-cr-00252 (D. Minn. Feb. 27, 2018), ECF No. 44 (same).

Nor is the government's conduct saved by the fact that it obtained a search warrant *after* illegally obtaining the Password. As an initial matter, an FBI agent failed to disclose in a sworn affidavit in support of the Devices Search Warrant that agents had improperly obtained the Password in violation of *Miranda*. Nor did the government disclose that the FBI intended to use the Password in order to "more efficiently" execute the search warrant on the Cellphone. Those material omissions defeat any possible claim that the search warrant somehow relieves the government from any meaningful remedy for the improper questioning of Dr. Ho. Moreover, obtaining judicial authorization to search does not thereby give the government license to then use illegal means to execute such a search. Indeed, the government's improper use of the Password to execute the search warrant constitutes an independent Fourth Amendment violation. *See United States v. Ramirez*, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of [a search] warrant." (internal citation omitted)); *Terebesi v. Torreso*, 764 F.3d 217, 235 (2d Cir. 2014) ("[T]he method used to execute a search warrant, [is], as a matter of clearly established constitutional law, subject to Fourth Amendment protections."). Accordingly, the defense respectfully submits that both Dr. Ho's post-arrest statement and any evidence obtained from the Cellphone must be suppressed.

POINT II

THE COURT SHOULD SUPPRESS ALL EMAILS OBTAINED PURSUANT TO SEARCH WARRANTS FOR CERTAIN EMAIL ACCOUNTS ISSUED IN THIS CASE AND ALL EVIDENCE DERIVED THEREFROM

Over twenty-one months after it first began obtaining search warrants returns containing the contents of five email accounts, the government still had not completed its review for

responsiveness to the warrants. These email accounts contain thousands of emails, including personal emails addressing topics ranging from the mundane to intimate details of Dr. Ho's personal life. The government's extraordinary delay in reviewing these emails for responsiveness—or stated another way, in carrying out what it said it would do when it first sought permission to search these email accounts—is unacceptable by any standard. It offends basic constitutional norms, and therefore blanket suppression is not only warranted—it is required.

Electronically stored information "can give the government possession of a vast trove of personal information about the person to whom the [information] belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure," and "the potential for privacy violations occasioned by an unbridled, exploratory search . . . is enormous." *United States v. Wey*, 256 F. Supp. 3d 355, 383 (S.D.N.Y. 2017). Because of the unique characteristics of electronically stored information, Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure provides that a warrant may authorize the government to, in the first instance, seize or copy such information in bulk, and then "later review . . . the information consistent with the warrant." *Id.*; *see also United States v. Metter*, 860 F. Supp. 2d 205, 214 (E.D.N.Y. 2012).

It is incumbent upon the government to include as part of its later review, however, a review of the search warrant returns for responsiveness. *See Wey*, 256 F. Supp. 3d at 383; *Metter*, 860 F. Supp. 2d at 215. That is, the government is required to review the search warrant returns to separate the data that is responsive to the search warrant from that data that is unresponsive to the search warrant. *See United States v. Debbi*, 244 F. Supp. 2d 235, 237–38 (S.D.N.Y. 2003); *Metter*, 860 F. Supp. 2d at 215. This procedure is distinct from government efforts merely to continue sifting through data to locate usable evidence. *See Wey*, 256 F. Supp.

3d at 405. Unresponsive data must then be placed outside the scope of subsequent government review, in order to avoid treating the search warrant as a general warrant. *See id.* at 406-07.

Of critical importance to this case, "Although 'there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence falls within the scope of a warrant,' courts have recognized that 'the Fourth Amendment requires the government to complete its review, *i.e.*, execute the warrant, within a "reasonable" period of time.'" *Wey*, 256 F. Supp. 3d at 383 (quoting *United States v. Metter*, 860 F. Supp. at 215); *United States v. Lustyik*, 57 F. Supp. 3d 213, 230 (S.D.N.Y. 2014) ("Like all activities governed by the Fourth Amendment, the execution of a search warrant must be reasonable," and "[l]aw enforcement officers therefore must execute a search warrant"—including, when applicable, review of recovered electronic communications—"within a reasonable time."); *cf. United States v. Ganias*, 824 F.3d 199, 209–10 (2d Cir. 2016) ("[T]he reasonableness of government conduct in executing a valid warrant . . . can present Fourth Amendment issues."); *Lauro v. Charles*, 219 F.3d 202, 209 (2d Cir. 2000) ("[T]he Fourth Amendment's proscription of unreasonable searches and seizures 'not only . . . prevent[s] searches and seizures that would be unreasonable if conducted at all, but also . . . ensure[s] reasonableness in the manner and scope of searches and seizures that are carried out." (elipses in original) (quoting *Ayeni v. Mottola*, 35 F.3d 680, 684 (2d Cir. 1994))).

Here, the government appears to have failed to review the emails obtained pursuant to the Email Search Warrants within a reasonable period of time. The government disclosed last month that as early as June 2016, it began to receive search warrant returns for the Email Accounts associated with Dr. Ho. *See* Government's March 23 Letter at 2. At least as of March 2018, however—*twenty-one months* after the government began to receive the search warrant returns—

the government had yet to complete its review of the materials for responsiveness to the Email Search Warrants. (*See* Letter to Hon. Katherine B. Forrest, Mar. 2, 2018, ECF No. 54 (noting that the government had retained a third-party vendor to assist in the review, and that such vendor was still in the process of completing its "initial" review).) In other words, at least as of twenty-one months since it first began receiving search warrant returns, the government had not executed the search warrants and was potentially still running searches through emails that should long ago have been segregated as unresponsive. Indeed, it is unknown whether the government has completed that review even as of the date of this motion.

This timeframe far exceeds the amount of time that other courts have held to be reasonable, *see, e.g.*, *United States v. Mutschelknaus*, 564 F. Supp. 2d 1072, 1077 (D.N.D. 2008) (finding a two-month delay to be reasonable), and in fact exceeds the amount of time that other courts have expressly held to be *unreasonable*. *See Metter*, 860 F. Supp. 2d at 215 (finding that "the government's more than fifteen-month delay in reviewing the seized electronic evidence" for responsiveness "constitute[d] an unreasonable seizure under the Fourth Amendment" that warranted blanket suppression); *cf. United States v. Ganias*, 755 F.3d 125, 140 (2d Cir. 2014), *reversed on reh'g en banc on other grounds*, 824 F.3d 199 (2d Cir. 2016) (concluding that the government retaining non-responsive files for a "prolonged period of time"—there, two-and-a-half years—violated the defendant's Fourth Amendment rights); *Debbi*, 244 F. Supp. at 237–38 (finding a Fourth Amendment violation where the government seized documents and "pick[ed] over them for months thereafter without determining which were actually evidence of the alleged crimes).

The government's conduct warrants suppression of the Email Search Warrants, and all evidence derived therefrom. "Government agents 'flagrantly disregard' the terms of a warrant so

that wholesale suppression is required only when (1) they effect a 'widespread seizure of items that were not within the scope of the warrant,' and (2) do not act in good faith." *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (internal citation omitted) (quoting *United States v. Matias*, 836 F.2d 744, 748 (2d Cir. 1988)). "The rationale for blanket suppression is that a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is essentially indistinguishable from a general search." *Id.* at 141. Such disregard of the terms of the search warrants is apparent here. Specifically, in each of the Email Search Warrants, the government was authorized to seize only a subset of data that constituted evidence, fruits, and/or instrumentalities of violations of 15 U.S.C. § 78dd-1, *et seq.* (the FCPA), 18 U.S.C. § 666 (bribery concerning programs receiving federal fund), 18 U.S.C. § 1956 (money laundering), 18 U.S.C. § 1957 (engaging in a financial transaction in criminally-derived property), and/or 26 U.S.C. § 7206 (subscribing to a false tax return), and/or an attempt and/or conspiracy to commit one or more of the same. *See, e.g.*, Kim Decl., Ex. I ¶ 3 ("June 16, 2016 Agent Affidavit"). The government's failure to conduct a responsiveness review in a timely manner necessarily means that it has seized, for an unreasonable period of time, countless personal emails that were not within the scope of the Email Search Warrants. Such a course of conduct renders each of the Email Search Warrants a general warrant. *See Ganias*, 755 F.3d at 139 ("If the Government could seize and retain non-responsive electronic records indefinitely . . . every warrant to search for particular electronic data would become, in essence, a general warrant.").

The defense is, of course, not in a position to know every shortcoming of the government's review procedures, since the government has declined to share more detailed information about its efforts to execute the Email Search Warrants. The government has not made clear, for example, whether it has in fact finished its responsiveness review even to this

day, nor has it answered the other questions raised by the defense on March 9, 2018. *See* Defense's March 9 Letter; Government's March 23 Letter. Nonetheless, based on the current record alone, the Court should suppress all emails obtained pursuant to the Email Search Warrants.

To the extent that the Court feels that additional information is necessary to rule on the present motion, the defense respectfully requests that the Court schedule an evidentiary hearing to investigate further the government's efforts to execute the Email Search Warrants.[5] See *Debbi*, 244 F.Supp.2d 235, 238–39 (scheduling an evidentiary hearing under similar circumstances, "at which counsel and the Court would have the opportunity to review the pertinent records, question the executing agents, and the like"). At such a hearing, the defense would seek to determine, among other things: (1) when the government began its responsiveness review of each set of search warrant returns; (2) when the government completed each of those reviews; (3) who conducted the reviews, and how they were conducted; and (4) to extent to which the reviewers were assiduous in their review.

[5] In addition to moving to suppress the emails in question, the defense also moves pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure for the return of such emails. Rule 41(g) provides an independent basis for an evidentiary hearing. *See* Fed. R. Crim. P. 41(g) ("The court must receive evidence on any factual issue necessary to decide the motion.").

Conclusion

For the reasons stated herein, the Court should suppress (1) a post-arrest statement made by Dr. Ho; (2) all evidence obtained from a Huawei cellular telephone recovered from Dr. Ho's luggage; and (3) all of the emails obtained pursuant to search warrants for certain email accounts issued in this case, and all evidence derived therefrom.

Dated: New York, New York
April 16, 2018

Respectfully submitted,

By: _____

KRIEGER KIM & LEWIN LLP
500 Fifth Avenue, 34th Floor
New York, New York 10110
Tel.: (212) 390-9550
Edward.Kim@KKLllp.com
Paul.Krieger@KKLllp.com
Jonathan.Bolz@KKLllp.com
Jon.Bodansky@KKLllp.com

DECHERT LLP
1095 Avenue of the Americas
New York, New York 10036
Tel.: (212) 698-3622
Fax: (212) 698-3599
andrew.levander@dechert.com
benjamin.rosenberg@dechert.com

Attorneys for Chi Ping Patrick Ho